Office of the Illinois State Fire Marshal
1035 Stevenson Drive • Springfield, IL 62703

Information Technology Division

☒ AGENCY DIRECTIVE	☐ DIVISION DIRECTIVE		DIRECTIVE NUMBER IT091410-1
☒ UNCLASSIFIED	☐ CLASSIFIED	☐ OTHER: _________	DATE ISSUED 9.14.10
CLASSIFICATION LEVEL ☐ FOUO (For Official Use Only)	☐ LES (Law Enforcement Sensitive)		EFFECTIVE DATE 10.1.10
SUBJECT OSFM IT PROCEDURES	DISTRIBUTION AGENCY WIDE		RESCINDS, AMENDS OR SPECIAL INSTRUCTIONS NA
RELATED STANDARDS	RELATED DOCUMENTS		RESCINDS, AMENDS OR SPECIAL INSTRUCTIONS NA

1. Service Requests

1.1. A service request consists of any activity which requires Information Systems resources to complete. Service requests include all moves, adds, changes, installations, help desk and problem calls.

1.2. All requests for service should be processed by e-mail to the Information Systems Request email account (sfm.infosysrequest@illinois.gov).

1.3. If e-mail is not available, users should call 217-785-1525.

1.4. If the users request cannot be addressed within one hour, IS Staff should reply to the user to inform them of the estimated date/time of service will be done.

1.5. All requests must be completed within one (1) business day of receipt unless specified for a future date. If the request cannot be completed in that time frame, the user should get a brief status report from IS staff on the request which includes an expected completion date.

1.6. Computer supplies such as printer cartridges, ribbons, paper, labels, forms, wrist rests, mouse pads, glare screens for monitors, special computer desks or tables, or any other such supplies are the responsibility of a cooperative effort between Information Services, store room personnel, and users. Program managers may stock supplies for their field staff. Please use the office supply process for standard supplies. Send an

Information Systems Request for IT related supplies (toner, disks, etc.). The appropriate purchase authorization forms will be completed by Information Systems staff.

2. Installs/Moves/Changes

2.1. All hardware moves/adds/changes must be entered into the inventory database. This information is to be forwarded using the appropriate to the Inventory contact at Shared Services – Corrections.

2.2. All planned infrastructure configuration changes must be approved using the Change Management process.

2.3. A Change Request must be completed and approved for all planned changes. A Change Requests must be completed to document all unplanned outages.

3. Employee Provisioning

3.1. A Computer Access form must be done whenever a new employee is hired and their start date is known. A new employee can be provisioned in two working days.

3.2. If new equipment is needed, substitute hardware may be used until the procurement is completed. There is a six to eight week delay for procurement. If no new equipment is needed, a new employee can be provisioned in two working days.

3.3. An Information Systems Request must be done whenever an employee separates from the agency and their last date is known. All IT equipment must be turned into Information Services before Employees separates from the agency.

4. IT Governance Process

4.1. This process is used for any project requiring the acquisition of outside resources to complete. The IT Governance process is used for all procurements which cannot be completed with an internal purchase authorization.

4.2. OSFM management suggests a new project or procurement. The user works with Information Systems management staff to develop a Project Initiation Request.

4.3. Proposal is reviewed by OSFM upper management. Approved proposals must be appropriately funded.

4.4. Information Systems management updates the IT Strategic Plan and agency project portfolio.

4.5. Information Systems management is responsible for performing all CMS governance and procurement processes.

5. Infrastructure

5.1. Network servers should not be restarted during working hours. If the server has suffered a critical error or has stopped, the server may be re-started. An outage report must be completed if this situation happens more than once for the same device.

5.2. Users should be notified when planned outages occur.

5.3. Users should be notified (if possible) about the nature and estimated duration of unplanned outages.

5.4. A change requests will be completed for all infrastructure configuration changes. These change requests must be approved by the IS Manager (or his designee) before the work is done.

5.5. Documentation is to be completed for all infrastructure assets. Information Systems staff is responsible for the preparation and maintenance of the documentation. All infrastructure documentation is confidential. Requests for this information must be approved by Information Systems manager.

6. Confidentiality

6.1. Information Systems staff has administrative rights to all computer assets.

6.2. Information Systems staff will maintain the confidentially of all information which they have access.

6.3. Division management retains governance over the data stored in their computer applications. Requests for access to their application must be approved by the appropriate division management.

6.4. Computer users are responsible for the confidentially data stored on their local computer hard drives. Users should take the appropriate steps to ensure that no unauthorized person can access the data stored on their computer.

7. Data Storage and Backup

7.1. All internal user data should be stored on network server storage on agency network storage. Network storage is backed up daily. Information Systems staff cannot be responsible for data not stored on the network.

7.2. All internal users are responsible to back-up the data files stored on their local computer.

7.3. All remote users should take appropriate steps to back-up their data files. Information Systems staff cannot be responsible for data not backed up appropriately.

7.4. There is no agency backup for remote users. Remote users should have standard backup software installed on their laptop. The backups should be done to an external USB device. It is the user's responsibility to make sure that their local data is backed up. It is also the user's responsibility to replicate any database information on their computers to their host computers in a timely manner.

8. Disaster Recovery

8.1. Information Systems management will be responsible for development and testing of an IS disaster recovery plan.

8.2. In the event of an IS disaster, management will follow the provisions of the current agency IS disaster recovery plan.

8.3. Information Systems Support staff will participate in all Disaster Recovery planning and recovery efforts in order to restore services to the agencies as efficiently and effectively as possible.

9. Computer Security

9.1. Information Systems management is responsible for the physical and data security of all hardware, software and application assets on the agency network.

9.2. Information Systems management is responsible for the patch management of all hardware, software, anti-virus and application assets on the agency network. Remote users are responsible for the patch management of their assigned hardware, software, and anti-virus assets.

9.3. Agency users are responsible for the physical security of all IT assets assigned to them.

9.3.1. Agency users are required to change their password every 60 days. The password complexity requirements are as follows:

9.3.1.1. They must have a minimum of eight (8) characters.

9.3.1.2. They must contain any three (3) of the following:

9.3.1.2.1. capital letter

9.3.1.2.2. lower case letter

9.3.1.2.3. special character

9.3.1.2.4. numeral

9.4. Agency users should lock their workstation if left unattended for longer than 15 minutes. You press the {Control}{Alt}{Delete} keys on the keyboard and select lock at the dialog box to complete this task.

9.5. Agency users are required to report perceived security problems to Information Systems staff immediately upon discovery.

9.6. Agency users are required to report all virus attacks to Information Systems staff immediately upon discovery.

9.7. All virus-infected email must be reported to the Help Desk immediately. Do not open suspicious attachments accompanied by emails even if you know the party who sent the message. CMS Network Support is responsible for scanning all email for viruses.

10. Computer Use

10.1. Agency computers must only be used for State of Illinois business. Agency computer resources may not be used for personal gain.

10.2. No games may be installed on OSFM computers. When games are discovered on state equipment, IS reserves the right to uninstall it.

10.3. No unapproved software may be installed on agency computers. Software must be approved by the OSFM Information Systems Manager or designee.

10.4. Information Systems Support staff will only work for 30 minutes in attempting to recover a desktop computer with a virus or spyware problem. If after 30 minutes the virus or spyware problem persists, Information Systems Support staff will make a best effort to back up the user's data files and then re-image the computer.

10.5. Information Systems Support may re-image any desktop computer found running unauthorized software.

10.6. It is the user's responsibility to remember all passwords for custom applications or data files. Information Systems Support will only make a best effort to recover any lost passwords.

10.7. All desktops will use a standard software image as determined by the End User Shared Services staff. Requests for special configurations are to be reviewed and approved by the appropriate Information Systems staff.

10.8. Users must not subscribe to non-work related web-site emails. Email users are responsible to delete any SPAM email received.

10.9. Information Systems Support will maintain the email network applications and desktop clients.

10.10. The Information Systems inventory control software captures all workstation hardware and software information into a central database. Please note that if you have any unauthorized software on your computer, it will show up in that database. Users will be warned about unauthorized software to remove it, or the computer will be re-imaged.

10.11. There is no expectation of privacy on any information stored on any agency computer resource or in the use of any agency computer resource.

11. Internet Policy

11.1. Employee access to the Internet is determined by the division managers.

11.2. Internet policies apply to all agency computer and internet connections types.

11.3. Employees shall not share the use of the agency Internet access with another person.

11.4. Employees shall not use agency Internet resources for personal gain.

11.5. Employees shall not use agency Internet resources to transmit or solicit vulgar, indecent, obscene or pornographic materials.

11.6. Employees shall not use agency Internet resources to transmit or solicit unlawful or illegal materials, including any materials that violate any U.S. law regarding the transmission of technical data or software.

11.7. Employees shall not use agency Internet resources to transmit or solicit libelous, abusive, harassing, threatening and/or otherwise objectionable materials of any kind or nature.

11.8. Failure to comply may be cause for the revocation of Internet privileges for that employee. Progressive disciplinary actions may be taken.

11.9. Any unsolicited, inappropriate materials received must be reported to the IS Manager immediately.

12. Computer Inventory

12.1. All State of Illinois property control policies and procedures will be strictly adhered to in their inventory practices. Information Systems staff will comply with the Data Security on State Computers Act (Public Act 93-036) in the proper disposal of computer equipment.

12.2. Information Systems will use appropriate disk-wiping software to thoroughly erase the hard drives of computers sent to property surplus in compliance with the Data Security on State Computers Act.

12.3. Information Services is responsible for all agency computer equipment in computer inventory.

12.4. Employees are responsible for the computer equipment assigned to them.

12.5. It is employee's responsibility to notify Information Services whenever any computer equipment is lost or stolen. An appropriate police report must be completed for all stolen equipment.

13. Enforcement of Policies

13.1. The OSFM will investigate any alleged abuses of its computer resources. If a part of the investigation indicates that computer privileges have been violated, OSFM may limit the access of employees found to be using computer systems improperly.

13.2. Employees are responsible for their own actions and if OSFM's computer policies are violated, employees will be subject to discipline, up and including termination. If criminal laws have been violated, law enforcement authorities will be notified.

13.3. The offense may be forwarded to the Office of Inspector General if the offense warrants.